8. RISK ANALYSIS METHODOLOGY

8.1 WHAT IS RISK ANALYSIS?

Risk Analysis is the technical process and procedures for identifying, characterizing, quantifying and evaluating hazards. It is widely used in industry and by federal agencies to support regulatory and resource allocation decisions. The analysis of risk, also called Risk Assessment (see definitions of terms in Ch.1 and in the Glossary, App. A), consists of two distinct phases: a qualitative step of hazard identification, characterization and ranking; and a quantitative risk evaluation entailing estimation of the occurrence probabilities and the consequences of hazardous events, including catastrophic ones. Following the quantification of risk, appropriate Risk Management options can be devised and considered, risk/benefit or cost analysis may be undertaken and Risk Management policies may be formulated and implemented. The main goals of Risk Management are to prevent the occurrence of accidents by reducing the probability of their occurrence (e.g., practice risk avoidance), to reduce the impacts of uncontrollable accidents (e.g., prepare and adopt emergency responses) and to transfer risk (e.g., via insurance coverage). Most personnel safety and operational/handling precautions and requirements at hazardous facilities (and hardware design reviews and approval for plants and critical equipment) are intended to prevent, reduce the frequency or probability of occurrence of hazardous events and to minimize their potential impacts.

Both normal operations and unforeseen conditions can lead to accidents which cannot be prevented or controlled. In such cases, the residual risk must be accepted and managed by preparing emergency response procedures (e.g., evacuation and medical response plans) to lessen the consequences of such accidents. Deterministic and worst case scenario analyses are often used to assess the scope and exposure impacts of improbable hazardous events with high consequences.

Several recent reports have discussed the role of technical risk assessment inputs to regulatory analysis and policy decision making.[1-3] Since Risk Assessment is a field where safety and loss prevention are the chief concerns, conservatism at various steps in the analysis has often been adopted as a prudent approach. Thus, conservative assumptions have been compounded sometimes in setting unnecessarily stringent regulatory standards and requirements. In practice, excessive conservatism and use of "worst case" analysis has served as a basis for over-design of critical facilities, and over-regulation of industry by setting unnecessarily strict license and permit requirements.[4,5] Several mission Agencies (such as DOD, NASA, DOE, EPA, USBM, OSHA, NIH, NRC) have developed their own risk analysis tools to carry out studies either in support of regulatory standards, criteria and policies or to enable safe operations. For the past few years, an Interagency Task Force for Risk Assessment, led by the NSF, has been working on uniform standards, to the extent possible and practical, for risk analysis methods and their use by federal Agencies charged with protecting the safety and health of the workers and the public. Some of these tools and approaches, whether developed specifically for space applications (Ch.9) or for licensing decisions (e.g., NRC regulations and studies),[8,15,16] are transferable to DOT/OCST for regulation and oversight of commercial launch activities.

Risk Assessment provides the information necessary for Risk Management decisions. Risk Management, in a regulatory context, requires the evaluation of the impact and effectiveness of safety standards and regulations to impose additional controls or relax existing ones.

8.2 RISK PERCEPTION AND RISK ACCEPTABILITY

Subjective judgment and documented societal bias against low probability/high consequence events may influence the outcome of a risk analysis. Perceptions of risk often differ from objective measures and may distort or politicize Risk Management decisions and their implementation. Public polls indicate that societal perception of risk for certain unfamiliar or incorrectly publicized activities is far out of proportion to the actual damage or risk measure (by factors of 10-100 greater than reality for motor, rail and aviation accidents, but by factors of >10, 000 for nuclear power and food coloring).[14] Risk conversion and compensating factors must often be applied to determine risk tolerance thresholds accurately to account for public bias against unfamiliar (x 10), catastrophic (x 30), involuntary (x 100), immediate vs. delayed consequence (x 30) and the uncontrollable (x 5-10) risk exposure.[17]

Different risk standards often apply in the workplace, in view of voluntary risk exposure and indemnification for risk to exposed workers; as opposed to public risk exposure where stricter standards apply to involuntary exposure. The general guide to work place risk standards is that occupational risk should be small compared to natural sources of risk. Some industrial and voluntary risks may be further decreased by strict enforcement or adequate implementation of known risk management and risk avoidance measures (e.g., wear seat belts, stop drinking alcohol or smoking). Therefore, some of these risks are controllable by the individual (e.g., do not fly, take the car to work or smoke), while others are not (e.g., severe floods, earthquakes and tsunamis).

Relative Risk Assessment is a common method of ranking risk exposure levels which enables decision makers to define acceptable risk thresholds and the range for unacceptably high exposure that would require Risk Management resources for reduction and prevention. As Figure 8-1 and Table 8-1 illustrate, there are de facto levels of socially tolerated (acceptable) levels of risk for either voluntary or involuntary exposure to a variety of hazardous factors and activities. Although regulators often strive to assess absolute levels of risk, the relative ranking of risks is an appropriate Risk Management strategy for resource allocation towards regulatory controls. Cost benefit analysis is often required to bring the burdens of risk control strategies to socially acceptable levels. Figure 8-1 and Tables 8-1 and 8-2 show estimated risk levels associated with natural and other (occupational, transportation, etc.) hazards that may lead to undesirable health effects and casualties. They show that risk levels vary greatly by causes of harm (chemical, mechanical, natural or man made), probability, degree of control, duration of exposure to the consequence (immediate, delayed, short or long-term), distribution (geographical, localized) in time and space, benefit to society vs. costs of risk reduction and consequence mitigation.

Table 8-1 shows the relative risk exposure to individuals as a casualty probability from various natural and regulated causes.[19] This table and its precursors in the literature[6,17] illustrate that the public voluntarily assumes risk levels which are 100 to 1,000 times larger than involuntary exposures to natural hazards and normal activities. These levels may be used as indicators of socially acceptable risk thresholds to compare when new regulatory standards are set. Note that risk exposure is normalized both to the population exposed and to the duration of the exposure. To compare the risk associated with each cause, consistent units must be used, such as fatalities or dollar loss per year, per 100,000 population, per event, per man year of exposure, etc.

Issues related to acceptable risk thresholds for regulatory purposes and for the public at large are often complex and controversial.[1- 5,17,19] The typical approach to establish risk acceptance criteria for involuntary risks to the public has been that fatality rates from the activity of interest should never exceed average death rates from natural causes (about 0.07 per 100,000 population, from all natural causes) and should be further lessened by risk control measures to the extent feasible and practical.[13]

The societal benefit and the cost trade-offs for risk reduction are widely used guides to set and justify risk acceptability limits. By comparing the risks and benefits associated with certain regulated activities, fair, balanced and consistent

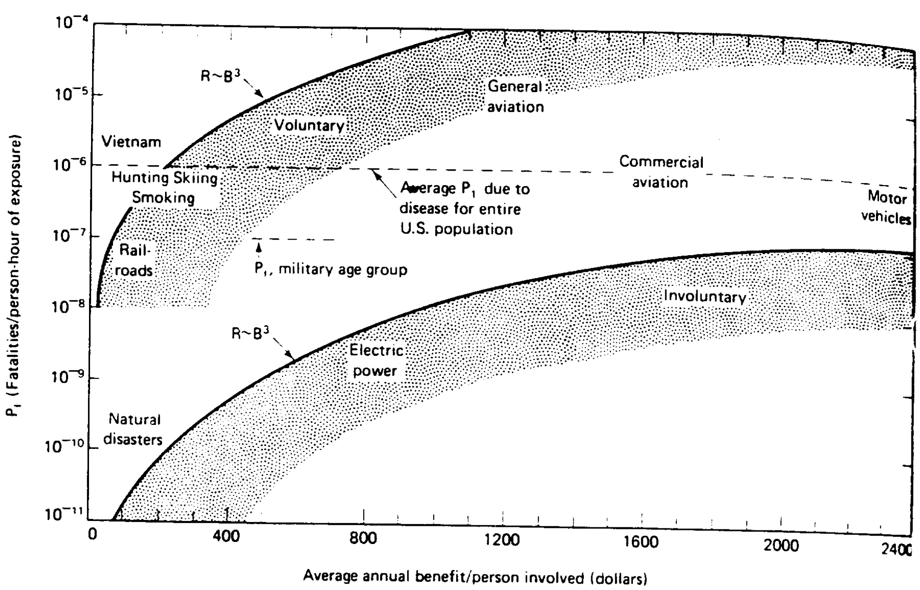


FIGURE 8-1. RISK VS BENEFITS (REF. 9)

TABLE 8-1. INDIVIDUAL RISK OF ACUTE FATALITY BY VARIOUS CAUSES. (REF. 19)

	ACTIVITY OR CAUSE	ANNUAL FATALITY RISK FOR EVERY 1 MILLION EXPOSED INDIVIDUALS
1.	Smoking (all causes)	3,000
2.	Motor vehicle accidents	243
3.	Work (all industries)	113
4.	Alcohol	50
5.	Using unvented space heater	27
6.	Working with ethylene oxide	26
7.	Swimming	22
8.	Servicing single piece wheel rims	14
9.	Aflatoxin (corn)	9
10.	Football	6
11.	Saccharin	5
12.	Fuel system in automobiles	5
13.	Lightning	0.5
14.	DES in cattle feed	0.3
15.	Uranium mill tailings (active sites)	0.02
	From all causes in U.S.	8,695
	From cancer in U.S.	1,833

* Indicates that the risk was regulated by the Federal government in the last 10 years. For these activities or causes, the risks in the table are estimates of risk prior to Federal regulation.

TABLE 8-2. ANNUAL RISK OF DEATH FROM SELECTED COMMON ACTIVITIES

	Number of deaths in representative year	Individual risk/year
Coal mining:		
Accident	180	1.3×10^{-3} or 1/770
Black lung disease	1,135	8×10^{-3} or 1/125
Fire fighting		8×10^{-4} or 1/1,250
Motor vehicle	46,000	2.2×10^{-4} or 1/4,500
Truck driving	400	10^{-4} or 1/10,000
Falls	16,339	7.7×10^{-5} or 1/13,000
Football (averaged over participants)		4×10^{-5} or 1/25,000
Home accidents	25,000	1.2×10^{-5} or 1/83,000
Bicycling (assuming one person per bicycle)	1,000	10^{-5} or 1/100,000
Air travel: one trans-continental trip/year		2×10^{-6} or 1/500,000

Source: Hutt, 1978, Food, Drug, Cosmetic Law Journal 33, 558-589.

limits for risk acceptability may be set and institutional controls on risk may be established. Figure 8-1 is based on Ref.9: Starr's 1969 risk benefit analysis, which, although later challenged in the literature, illustrates several general trends derived from an analysis of fatalities per person hour of exposure to natural hazards and to hazardous human activities, in terms of dollar-equivalent benefit to society. It appears that voluntarily assumed risk levels are a factor of about 1,000 higher than involuntary risk exposure levels over the entire range of benefits. Also, the acceptable risk curve appears to vary as the cube power of the benefit, on this log-normal scale.

A typical regulatory risk threshold used to institute controls is the one-in-a-million casualty probability.[17] Situations at this threshold include: traveling 60 miles by car or 400 miles by air, two weeks of skiing, 1.5 weeks of factory work, 3 hours of work in a coal mine, smoking one cigarette, 1.5 minutes of rock climbing and 20 minutes of being a man aged 60.

By analogy with other industries, in the case of space operations, Range personnel and commercial launch service firms may be considered voluntary risk takers, while the public at large is involuntarily exposed to launch and overflight risks. While Range Safety and on-site Range personnel are highly trained in risk avoidance and management, the public must be exposed to only minimal risk from commercial launch activities.

There are clear but indirect public, economic and other societal benefits derived from commercial space operations, including efficient telephone and video communications, weather forecasting, remote environmental sensing and crop data, better drugs, advanced material fabrication, superior navigation capability and other technology spin-offs. Based on the risk comparability approach illustrated in Ch. 5 (Vol. 2) and the Range Safety controls and practices (Chs. 2, Vol. 1 and 9, 10), commercial launch activities appear to be well within the socially acceptable risk limits at this time.

8.3 EXPECTED RISK VALUES AND RISK PROFILES

There are two fundamental components of Risk Analysis:

- Determination of the probability, P_i (or frequency of occurrence, f_i), of an undesirable event, E_i. The probability of an event is its likelihood of occurrence or recurrence. Sometimes the probability estimates are generated from a detailed analysis of past experience and historical data available; sometimes they are judgmental estimates on the basis of an expert's view of the situation or simply a best guess. This quantification of event probabilities can be useful, but the confidence in such estimates depends on the quality of the data base on actual failures and the methods used to determine event probabilities. Probabilities have long been used in the analysis of system reliability for complex equipment and facilities and to anticipate and control various failure scenarios.

- Evaluation of the consequence, C_i, of this hazardous event: The choice of the type of consequence of interest may affect the acceptability threshold and the tolerance level for risk.

The analytical phase of a Risk Analysis generally consists of three steps:[10] The triad: event (scenario), probability and consequence is sometimes called the "Risk Triplet."

1. The qualitative step involves the selection of specific hazardous reference events E_i (hazard identification) or scenarios (chains of events) for quantitative analysis.

2. The quantitative analysis requires the estimation of the probability of these events, P_i.

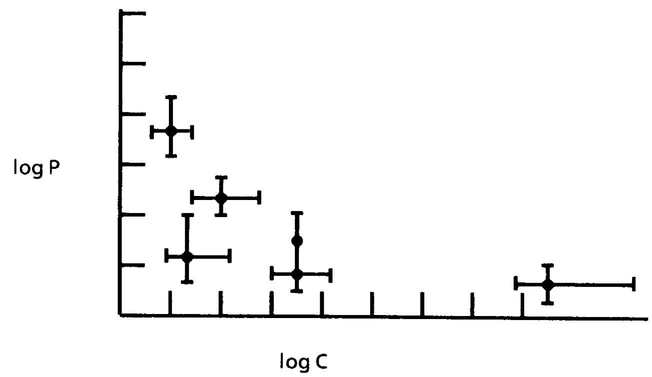
3. The next quantification step is to estimate of the consequences of these events, C_i.

The results of the analytical phase are used in the interpretive phase in which the various contributors to risk are compared, ranked and placed in perspective. This interpretive phase consists of:

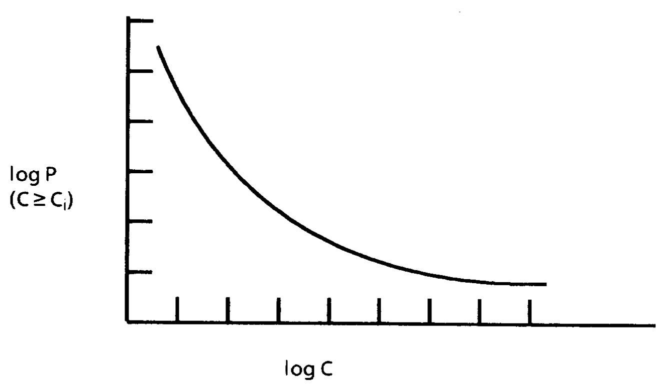
4. The calculation and graphic display of a Risk Profile based on individual failure event risks. The process is presented in Figure 8-2.

5. The calculation of a total expected risk value (R) by summing individual event contributions to risk (R_i).

Naturally, all the calculations undertaken involve some uncertainties, approximations and assumptions. Therefore, uncertainties must be considered explicitly. Using expected losses and the risk profile to evaluate the amount of investment that is reasonable to control risks, alternative Risk Management decisions involving avoidance (i.e. probability decrease) or consequence mitigation can be evaluated in terms that are useful to the decision maker.



(a) Plotting of points corresponding to individual failure events. Logarithmic scales usually used because of wide range in values. The error brackets denote uncertainties in probability estimates (vertical) and in anticipated consequences (horizontal) for each failure mode/event.



(b)Construction of the cumulative probability risk profile curve (as described in text)

FIGURE 8-2. CONSTRUCTION OF A RISK PROFILE

Therefore, a sixth planning step usually included in Risk Analysis is:

6. The identification of cost effective Risk Management options, to be followed by:

7. Adoption of a Risk Management policy and implementation.

The analytical phase yields results in the general form suggested in Table 8-3. There are two useful ways to then interpret such results: expected risk values, R_i, and risk profiles. Both methods are employed for quantitative risk analysis.

TABLE 8-3. GENERAL FORM OF OUTPUT FROM THE ANALYTIC PHASE OF RISK ANALYSIS

UNDESIRABLE EVENT	PROBABILITY* +	CONSEQUENCES** +	RISK LEVEL
E_1	P_1	C_1	$R_1 = P_1C_1$
E_2	P_2	C_2	$R_2 = P_2C_2$
E_3	P_3	C_3	$R_3 = P_3C_3$
.	.	.	.
.	.	.	.
E_N	P_N	C_N	$R_N = P_NC_N$

*Probability of an event is expressed as a fraction, or in percent (dimensionless). Alternatively, a frequency per year, or per event (in units of 1/time) may be used.

**Consequence, in the case of an accident is a measure of the accident impacts of interest to the analysis (e.g. mission loss, payload damage, damage to property, number of injuries, dollar loss, etc.)

+ Usually point values estimates for P_i and C_i are bracketed by best case - worst case estimates, to indicate the residual uncertainty in point estimates. Orders of magnitude in the range bracketing consequence and probability estimates are not uncommon, as the brackets in Fig.8-2 show.

Expected values are most useful when the consequences C_i are measured in financial terms or other directly measurable units. The expected risk value R_i (or expected loss) associated with event E_i is the product of its probability P_i and consequence values:

$$R_i = P_i x C_i$$

Thus, if the event occurs with probability 0.01 in a given year, and if the associated loss is one million dollars, then the expected loss is:

$$R_i = 0.01 \text{ x } \$1{,}000{,}000 = \$10{,}000$$

Since this is the expected annual loss, the total expected loss over 20 years (assuming constant $) would be roughly $200,000. This assumes that the parameters do not vary significantly with time and ignores the low probability of multiple losses over the period. To obtain the total expected loss per year for a whole set of possible events, simply sum the individual expected losses:

$$\text{Total Risk, } R_T = P_iC_i + P_2C_2 + \quad . \quad . \quad + P_NC_N =$$

$$= \sum_{i=1}^{N} P_i C_i = \sum_{i=1}^{N} R_i$$

This expected risk value assumes that all events (E_i) contributing to risk exposure have equal weight. Occasionally, for risk decisions, value factors (weighting factors) are assigned to each event contributing to risk. The relative values of the terms associated with the different hazardous events give a useful measure of their relative importance and the total risk value can be interpreted as the average or "expected" level of loss to be experienced over a period of time. One particular way in which it is used is to compare it to the cost of eliminating or reducing risk (i.e., as part of the Risk Management strategy) in the context of cost/benefit analysis. Expected values of risk (R) are of prime importance in both business and in regulatory decision making under complex and uncertain situations.

Based on the definition of expected values, if event E_2 has ten times the consequences of event E_1 but only one tenth the likelihood, then the products $R_1 = P_1C_1$ and $R_2 = P_2C_2$ are equal. That is, the events have the same expected level of risk. Thus, expected risk levels provide a balance of probabilities and consequences. In mathematical terms, the expected values may be similar, but the low probability, high consequence event may be of greater concern.[11,12] For example, a company may be prepared to sustain a steady level of relatively small losses or accidents, but is concerned with guarding against truly catastrophic events. This is the motivation behind Risk Management, although, in all cases a range of consequences may be of interest. Determining the point estimates for best and worst case R_i will produce limiting values for the risk estimates and yield a band of uncertainty in risk level.

A common way to interpret the values of probabilities and consequences of different hazardous events is by means of a Risk Profile. This displays the probability distribution for accidents and the range of their severity as a function of likelihood. If sufficient accident data exist, the cumulative probability distribution function is used as a Risk Profile to show the probability of damages at a given level or greater. Figure 8-3 shows an example of a hypothetical Risk Profile for commercial launch operations. A point (P_i, C_i) on the curve can be interpreted to mean there is a probability, P_i, of an accident with a consequence at least as large as C_i. Given a set of ordered pairs (P_i, C_i) obtained during the analytic phase of a risk study, the actual Risk Profile is computed using the laws of probabilities and combinatorial analysis. For actual cases, the risk profile is usually constructed by drawing the lowest decreasing curve so that all the points with $C \leq C_i$ are on or below it. The separate hazardous events with consequences $C_i \leq C$ are combined into a single event with a probability equal to the sum of their individual probability values (i.e., their cumulative probability). Then, the ordinate value P_i in Figures 8-2 and 8-3 indicates the probability of an event, E_i, with a consequence as large as or exceeding C_i ($C \geq C_i$). The acceptability ranges for risk must be determined and regulatory risk targets must be set consistent with these acceptable risk thresholds. These goals are often set according to ALAP (as low as practical), BAT (best available technology), BPT (best practical technology) or the cost of risk reduction.[17] The relative risk reduction achieved by various controls is also displayed on the Risk Profile to indicate the merit and effectiveness of potential regulatory risk reduction measures.

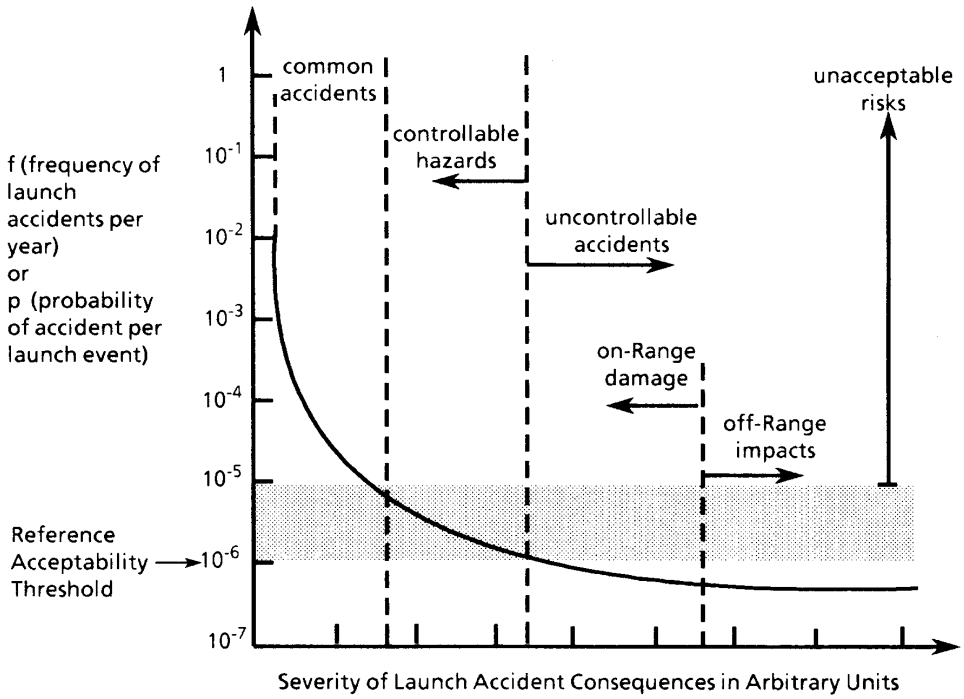


FIGURE 8-3. A SCHEMATIC RISK PROFILE FOR COMMERCIAL ELV OPERATIONS

The frequency or the probability of the undesirable event (launch accidents) is plotted against the consequence magnitude of interest (potential public safety impacts such as dollar loss for property damage, casualty, insurance claims). The shape of the curve could be convex, rather than concave, or even discontinuous, depending on the scale and the data points available. Shaded area denotes de-facto acceptable risk levels or design/operation safety goals based on established ELV launch practices at Government Ranges.

8.4 IDENTIFICATION OF HAZARDS, PROBABILITY ESTIMATION AND CONSEQUENCE MODELING

Fault tree (or event tree) analysis has been successfully applied in many technical fields to identify and logically order scenarios leading to equipment breakdown, financial loss or other system failures to be controlled (see section 8.7). Fault trees have been applied occasionally to problems associated with space launches, mission planning and approval (Chapters 9 and 10). This results in an extensive set of analyses of the potential launch failure events and consequences.

Consequences of observed or anticipated accidents are often modeled by extrapolation from small scale tests, limited observations, simulations and scoping calculations. The goal of quantitative risk assessment is not only to identify and rank hazards, but to analyze the low probability events of high consequence. This can focus corrective action, improve management of risk factors and optimize resource allocation. These extreme events are feared most by both public and regulators. They are often used as "worst case scenarios" or extreme "catastrophic" failures that serve as the basis for conservative design and regulatory requirements.[11,12]

However, catastrophic failures are seldom observed. Therefore, their probability of occurrence and consequences are uncertain and difficult to quantify. The Three Mile Island nuclear reactor accident was this type of rare event. It occurred after 500 reactor years without a significant accident, yet was qualitatively anticipated and approximated. A severe earthquake along the San Andreas Fault, with catastrophic impacts on the San Francisco Bay area, is another example of an anticipated hazard of low probability and high consequence that is difficult to predict and control. Future levels of risk are usually predicted by statistical analyses of relevant experience, although, a complete time series and representative sampling of hazardous events seldom exists. Predictions are often based on inference, event reconstruction, interpretation and extrapolation, rather than on observed events.[11] Because industry and regulators learn to improve safety and reduce risk based on prior experience, Bayesian statistics are sometimes used to reflect the decrease in the probability/frequency of hazardous events when "learning" improves the odds.[11,13] Alternative computational methods to infer a risk profile envelope have been developed (e.g., trend analysis) that include low probability, high consequence events, when the high consequence results from a number of intermediate events and the structure of such a composite event can be analyzed and quantified.[12] However, such predicted or composite risk profiles are often controversial, as is discussed in Chapter 9, which reviews the application of Risk Assessment methods to space launch and orbiter systems and missions.

8.5 UNCERTAINTIES AND RELIABILITY

Risk Analysis is not an exact science. Despite this, it is widely used to support regulatory and industrial decision making and to allot resources. Risk analyses performed by different analysts on the same issue may lead to different results. The reason is that there are substantial uncertainties intrinsic to risk assessments deriving from incomplete knowledge and identification of potential failures, from incorrect modeling assumptions used in the quantification of hazardous events or, more likely, from the variability in the possible type, time, place and circumstances of an accident. Different (and possibly incomplete) data bases and assumed failure rates of components may be used and thus lead to discrepancies in results. Different statistical analyses of the same data base may be justified by stated assumptions and lead to further discrepancies in results. Furthermore, the choice of a certain risk analysis methodology may influence, and even determine, the conclusions of the analyses. Judgments by experts evaluating and ranking the hazards, i.e. the Delphi approach, are often subjective. Hence, the risk analysis process has inherent limitations and uncertainties which must be taken into consideration in decision making.

Tests to establish reliability of complex components or systems are usually expensive, making a minimum of tests desirable. On the other hand, true probabilities are based ideally on results from very large samples. When only a few items are tested, the results may not be truly representative. Tossing a normal coin two or three times may result in heads each time. This may lead to the erroneous assumption that the result will always be heads. The next three tosses may all be heads again, all tails or combinations of heads or tails. With more and more tests the average probability of a head (or tail) will be found to approach 0.5. The problem then arises as to how much confidence can be placed on past results to predict future performance. The term confidence level is used for this purpose. Tables have been prepared to indicate the relationships between test results, reliability and confidence. One such table is shown below in abbreviated form (Table 8-4).

Since there are residual uncertainties associated with the quantification of risk, confidence limits must be placed both on failure probabilities (usually 60%-90% brackets) to reflect this uncertainty. A 60 percent confidence interval means that there is a 60 percent chance that the actual failure rate falls within the range of given estimates. A 90 percent confidence limit means that there is a 90 percent chance that real events will fall within an estimated range. Confidence limits are based on observations: if no failures occurred in 1,000 trials, there are still three failures possible in the next 1,000. If 10,000 tests were successfully completed, that would statistically correspond to a probability of three failures in 10,000 events with 95 percent confidence (i.e., a reliability of .9997). In addition, there may be large uncertainties in the consequence estimate, so that for any "best guess" point estimate, "worst case" and "best case" limits are needed.

TABLE 8-4. NUMBER OF TESTS THAT MUST BE PERFORMED WITHOUT A FAILURE TO PROVIDE A SPECIFIC MINIMUM RELIABILITY AT ANY CONFIDENCE LEVEL. (Ref. 6)

MINIMUM RELIABILITY (%)	CONFIDENCE LEVEL 90%	95%	97 1/2%	99%	99 1/2%
75	8	11	13	16	19
80	11	14	17	21	24
85	15	19	23	29	33
90	22	29	35	44	51
95	45	59	72	90	103
96	57	74	91	113	130
97	76	99	122	152	174
98	115	149	184	229	263
99	230	299	370	460	530

Most assemblies and systems actually do not have constant failure rates, especially when the system does not have many components that are similar or have similar characteristics, such as large mechanical units. Instead of being exponential, the distribution of failures may be Gaussian, Weibull, gamma or log normal. The chief difference is in establishment of failure rates. Means of improving reliability as indicated above remain the same. Table 8-4 is based on the simplest assumption of a binomial distribution, where the outcome of any trial can be either failure (F) or success (S), randomly occurring with the probability of .5 (like tossing coins for Head/Tail outcomes).

8.6 RELIABILITY VERSUS SAFETY

Reliability Analysis often provides useful inputs to quantitative safety analysis since failure rates (observed or design goals) for safety critical components and subsystems permit the evaluation and control of adverse safety impacts. Often, to ensure safe operation, safeguards are incorporated into system engineering design, such as: redundant features; manual overrides for automatic components (valves, switches) which are safety critical and special quality assurance, acceptability and maintainability specifications. Space launch vehicles and payloads have been traditionally provided with redundancy in the in-flight destruct or other termination system and the flight control and communications subsystems (see Chapter 2, Vol.1). This ensures that a guidance failure or a failure in boost, sustainer or upper rocket stages will not lead to undesirable off-range risk exposure and that risk to the public will be avoided and controlled by the Range Safety Officer's ability to safely destroy the spacecraft on command.

Reliability data on components and subsystems are essential to predicting performance. Table 8-5 shows as an example the estimated probability that a certain number of failures will occur in the next 20 tries for a hypothetical launch vehicle, based on assumed operational performance reliability figures in the range of historical values and on a skewed binomial distribution. (See also Ch.3, Vol. 1 for published reliability figures on commercial space vehicles.)

TABLE 8-5. RELIABILITY USED AS PERFORMANCE PREDICTOR FOR A HYPOTHETICAL LAUNCH VEHICLE

	VEHICLE RELIABILITY (R)				
	0.98	0.975	0.97	0.96	0.95
EXPECTED "EVENT" (NUMBER OF LAUNCH FAILURES IN 20 TRIES)	PROBABILITY OF EVENT (P PERCENT)*				
0	67	60	54	44	36
1	27	29	34	37	38
2	5	6	10	15	19
3	<1	1	2	4	6
4	0	0	0	0	>1

An illustration of the use of binomial distribution skewed to higher probability of the "event," defined as "x failures in the next 20 consecutive launches." Note that the higher the assumed reliability, the higher the probability of "sucess" (i.e., fewer failures in 20 launch attempts).

However, it must be noted that although reliability figures feed safety analyses directly, a highly reliable system is not necessarily safer. A key issue is the trade off between reliability and safety: adding sensors and control systems to detect malfunctions in a critical subsystem may enhance safety, but decrease the overall reliability. A stick of dynamite is an example of a highly reliable, but clearly unsafe object: when triggered intentionally or unintentionally, it will explode reliably. It is unsafe because of its high energy content, its explosive potential and its low trigger threshold. Safeguards may enhance handling safety, but decrease functional reliability. In favor of the reliability of simplicity, some engineers would trade the sophisticated injection pumps in modern rockets for simple gravity fed ("big dumb") rockets.

Both human error and infrequent operational or accidental failures, can lead to catastrophic accidents with a low probability of occurrence and potentially high risk exposure. Indeed, in the case of space launch systems and operations, it is the low probability and high consequence event that would dominate the public risk exposure. The likelihood of occurrence and the public safety impacts of any accidental failure in such highly reliable subsystems and systems must be quantitatively assessed in order to appropriately define acceptable and expected levels of risk, and to regulate commercial space activities via the licensing process (see Chapters 9 and 10).

Table 8-6 shows the kind of basic component failure rates which are used in probabilistic system failure computations. These apply to all mechanical and electrical systems across industries. Similarly, human error must often be factored into estimating probabilities of systems breakdown, since operator error or judgment errors in responding to minor failures can have major consequences. Table 8-7 shows that high stress work conditions lead to more frequent human error than routine functions and operations. Human failure rates are typically higher than equipment failure rates and may compound them because of improper or incomplete operator training in recognizing critical situations or because of panic/stress response to an accident. Considerable attention has been paid to human/ machine interfaces and to crisis training of personnel. The same considerations should apply in analyzing a launch "go/no go" decision, or a command destruct decision for a space system, as for a reactor operator or a flight controller in a busy airport tower.

TABLE 8-6. COMPONENT FAILURE RATES

Automatic Shutdown	10^{-2}/demand
Emergency Shutdown System	10^{-3}/demand
Defective Materials (Seals)	10^{-4}/demand
Defective Pumps	10^{-3}/year
Faulty Gasket	10^{-5}/year
Brittle Fracture (pipes)	10^{-5}/year
Pipe Failure - 3' rupture	8×10^{-5}/section year
Spontaneous Failures (tanks, etc)	10^{-6}/year

TABLE 8-7. HUMAN FAILURE RATES (Ref. 18)

Task	Probability of Error/Task
Critical Routine	10^{-3}
Non-critical Routine: errors of omission and commission	$10^{-2} - 10^{-3}$
High Stress Operations.	$10^{-2} - 10^{-1}$
Responses after major accident during:	
- 1st minute	1
- to + 5 minutes	9×10^{-1}
- to + 30 minutes	10^{-1}
- to + several hours	10^{-2}

8.7 RISK ASSESSMENT METHODS

The adoption of an appropriate analytical technique is important to any meaningful qualitative or quantitative failure and/or risk analysis. Each risk quantification method discussed and illustrated below has its own special merits, strengths, weaknesses and an optimal domain of application (see Table 8-8). Only if sufficient empirical and statistical data are available is the probabilistic modeling of hazardous events justified. For the very infrequent catastrophic event, a deterministic analysis of consequences (i.e., scoping calculations to estimate the type and magnitude of impacts assuming that the accident has occurred) may be sufficient in order to consider possible risk management (prevention and emergency response) and to estimate the associated sensitivity to assumptions. Deterministic consequence modeling of an unlikely catastrophic event is acceptable and even necessary whenever accident statistical and heuristic data available do not suffice to justify quantitative estimates for its occurrence and observation based scoping estimates for the magnitude of its consequences.

TABLE 8-8. STRENGTHS AND WEAKNESSES OF SELECTED RISK QUANTIFICATION TECHNIQUES (REF. 10)

STRENGTHS	WEAKNESSES
Preliminary Hazard Analysis (PHA)	
• May be applied during very early stages of project development. • Very straightforward to carry out. • Provides documentation of results.	• Difficult to show effects of mitigation or to prioritize the causes of one undesired outcome as does not show multiple causes of undesired event in same place. • Not particularly useful at later stages of development or for reanalysis.
Fault Tree Analysis (FTA)	
• Logical presentation of event sequences of concern. • Shows relative significance of events and causes. • Readily demonstrates effectiveness of mitigation or redesign. • Can be used in sensitivity analyses. • Can cover human errors as well as equipment failures.	• Time consuming and requires careful identification of both top events and causes. • Requires skill to handle common mode failures, dependent events, and time dependencies. • May be difficult to justify/obtain probabilities needed for quantification.
Event Tree Analysis (ETA)	
• May be used to develop critical events and consequences by starting with a single failure, or may start with critical event and develop consequences. • Orders events in time sequence in which they occur. • Displays logical relationships.	• May need FTA or some other method to develop probabilities. • Very time consuming if starting with individual failures. • May be incomplete if all events not identified. • Difficult to handle partial failures or time delays.

There are several inductive methods of risk analysis which assume a particular failure mode or failure initiating event. The effects on the system performance are then analyzed in order to infer the propagation of failures (failure chains) and to assess the sensitivity of the system operation to the postulated initial failures (bottom to top). The methods listed below focus primarily on hazard identification and on the probabilities of occurrence of hazardous events:

Inductive risk analyses methods used in industry to determine what failed states are possible include:

- The Preliminary Hazards Analysis (PHA) - This is the most general and qualitative identification and listing of potentially hazardous conditions, which is used to guide design, or the definition of procedural safeguards for controlling these. Often, PHA suffices to identify causal failure chains, possible safeguards and risk prevention options.

  The list of hazardous events to be prevented or controlled can be developed into subevents. PHA is usually carried out at an early stage of design and operations planning in order to allow both design and operational controls to be implemented in a cost-effective manner. Table 8-9 is an example of a Preliminary Hazard Analysis list of failures/malfunctions, used to identify safety critical failures and hazardous conditions and consequences, used to suggest risk control (prevention, reduction and avoidance) strategies. The PHA technique has been used primarily in the chemical and petroleum industries and in the design of critical facilities.

The PHA, although chiefly an inductive method, can also be used in deductive analysis since it is primarily a systematic and hierarchical listing of failures, accidental events and circumstances leading to potentially catastrophic or major undesirable consequences. Such listing of failure events and their enabling conditions simulates closely and is complementary to a FTA (see below) since it permits the definition of hazardous chains of events and affords insight in the initiating (i.e., causal) factors enabling failure. The unlikely adverse end event can also be analyzed in terms of more probable subevents, down to the common minor failures in the domain of daily occurrences.

TABLE 8-9. MALFUNCTIONS AND FAILURES (REF. 6)

POSSIBLE EFFECTS	POSSIBLE CAUSES
Mechanical malfunctions Equipment will not operate Vibration and noise Bearing problems	Broken part Separation of couplings Separation of fasteners Failure to release holding device or interlock Binding due to heavy corrosion or contamination Misalignment of parts Misaligned, loose, or broken rotating or reciprocating equipment or parts Broken or worn out vibration isolators or shock absorbers Bearings worn due to overloading Bearings too tight or too loose Lack of lubrication
Power source failure Complete inactivation of power dependent systems Lack of propulsion during a critical period Guidance failure of a moving vehicle Failure during flight airborne systems Inability to activate other systems Failure of life support systems Failure of safety monitoring and warning systems Failure of emergency or rescue systems	Prime mover failure Internal combustion unit – Fuel exhaustion or lack – Oxygen exhaustion or lack – Lack or failure of ignition source for chemical reaction – Interference with reaction – Mechanical malfunction – Failure of the cooling system – Failure of the lubricating system Blockage of steam, gas or water used to drive turbines Excessive wear of power equipment Mechanical damage to power equipment Poor adjustment of critical device Failure of connection to electric generator Excessive speed due to lack of control Loss of electrolyte for battery or fuel cell
Electrical system Failure Entire system inoperative Specific equipment will not operate Interruption of communications Detection and warning devices inactivated Failure of lighting systems Release of holding devices	Faulty connector or connection Failure to make connection Conductor cut Fuses, circuits breakers, or cutouts open Conductor burned our Switch or other device open or broken Short circuit Overloading

- The Failure Mode and Effect Analysis (FMEA) - This is a more detailed analytical procedure, which is used to identify critical and non-critical failure modes. Single point (component) failures which can lead to system break down are thus identified and fixes, such as redundancies or operational bypass, are designed into the systems to prevent them. FMEA can be quantified if failure probabilities for components can be used to derive the percentage of failures by mode. Critical and non-critical effects are used for managing risk and preparing emergency response plans.

- Failure Mode Effect and Criticality Analysis (FMECA) - This type of analysis is a more detailed variant of FMEA. It is used for system safety analysis, to enable detailed assessment and ranking of critical malfunctions and equipment failures and to devise assurances and controls to limit the impacts of such failures (i.e. risk management strategies). FMECA is usually a tabular listing of: identified faults, their potential effects, existing or required compensation and control procedures, and a summary of findings.

- Fault Hazard Analysis (FHA) - This method is particularly useful for inter-organizational projects that require integration, tracking and accountability. It is typically used for space systems when numerous contractors design, test and certify various subsystems which must be integrated into a payload or a final launch system. FHA forms display in column format: the component identification by subsystem; a failure probability; all possible failure modes; the percent failures by mode; the effect of failures, up to subsystem interfaces; the identification of upstream components that initiate, command or control the failure and any secondary failure factors or environmental conditions to which the component is sensitive.

- Event Tree Analysis (ETA) - This approach is equivalent to the qualitative part of Fault Tree Analysis (FTA, see below) and is used to display the likely propagation of failures in a system. Figure 8-4 is an example of an Event Tree which is used to isolate a failure propagation sequence and identify enabling conditions which can be controlled. Event trees are used in FMEA, FMECA and FTA and require identification of all failure initiating events. Figure 8-5 is an example of an event tree for commercial space operational failures.

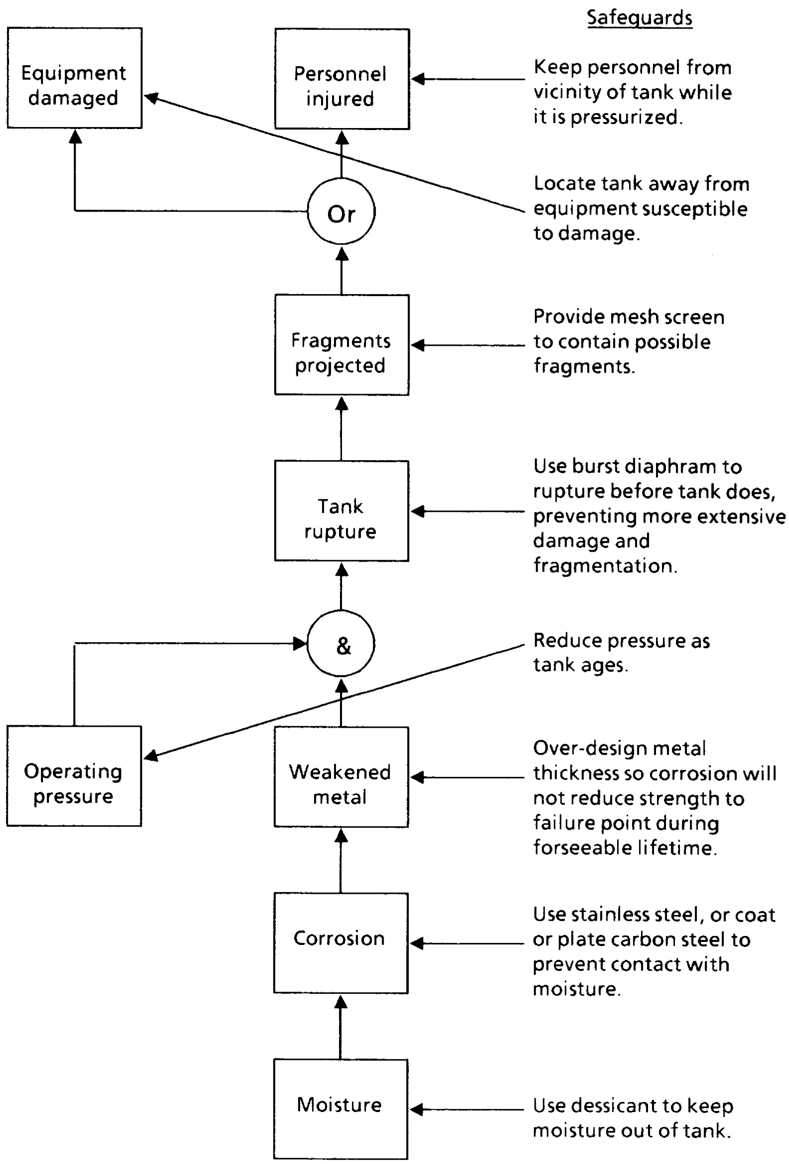


FIGURE 8-4. SEQUENCE OF EVENTS LEADING TO RUPTURE OF A PRESSURIZED TANK (Ref. 6)

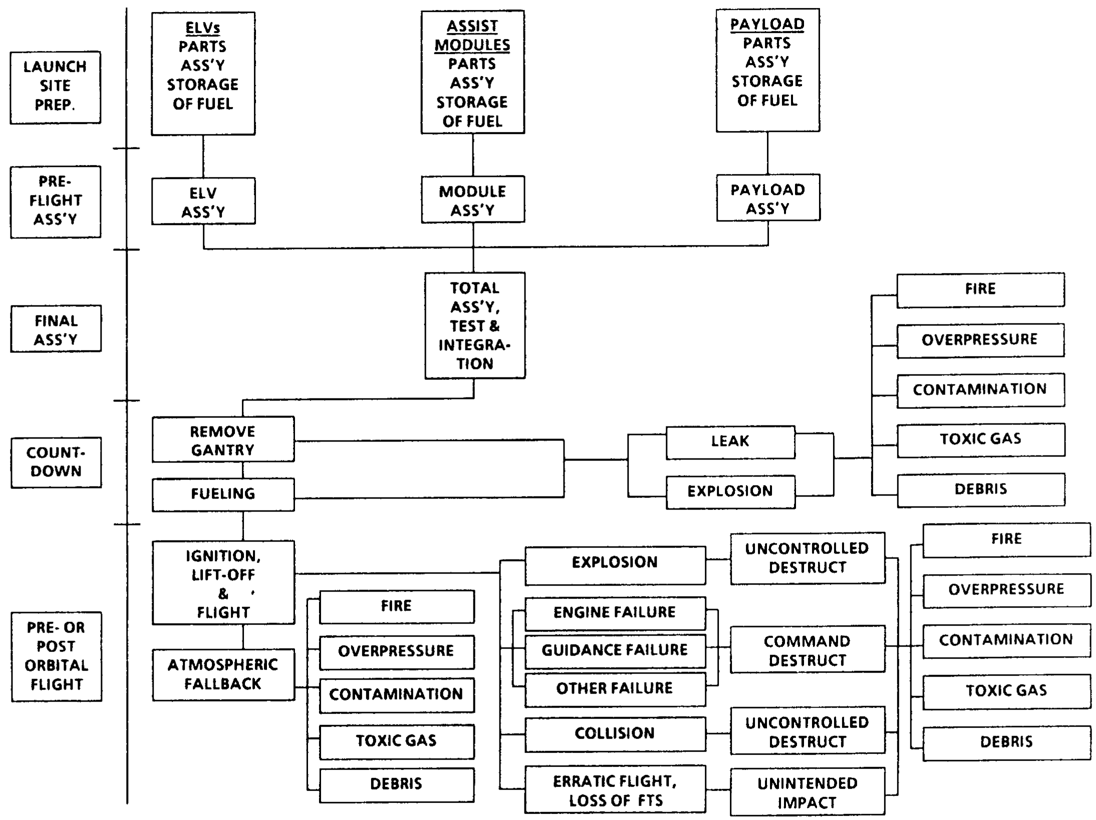


FIGURE 8-5. EVENT TREE FOR COMMERCIAL SPACE LAUNCH OPERATIONS

- Double Failure Matrix (DFM) - This method is used to list single vs. double subsystem failures, only after failure categorization by effects on the system have been completed. Namely, Fault Categories I-IV correspond to the severity of impacts on the system: I. negligible, II. marginal, III. critical and IV. catastrophic. Then, for each subsystem the component failures and the corresponding fault categories are listed in matrix form to determine how many ways a certain hazard category can occur (single and multiple failure modes).

- Hazard and Operability Analysis (Haz-Op), or Operability Hazard Analysis (OHA) - This is another method of safety analysis widely applied in designing complex chemical facilities.[10] This procedure involves the examination of design, piping and instrument diagrams (P&ID) and operation flow charts in order to ask a "what if" question at each node. What would happen if a deviation from normal operations and design conditions occurs at this point (Figure 8-6)?

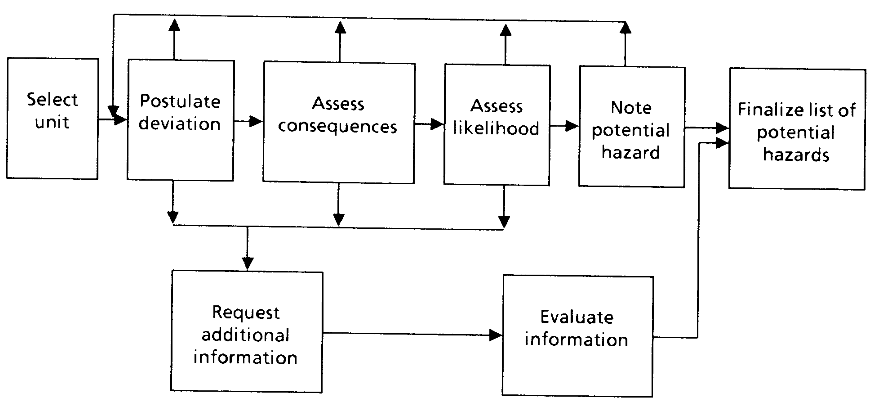
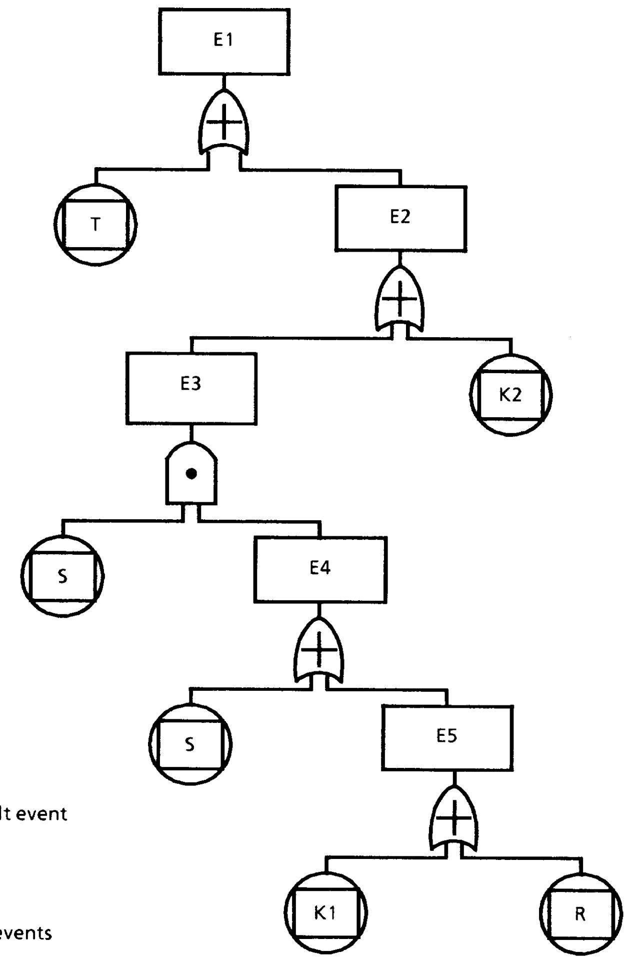


FIGURE 8-6. HAZ-OP METHODOLOGY (REF. 10)

This method is equivalent to the FMEA analysis in the sense that it permits identification of critical failure initiators, single point failures, malfunction chains and their effects on other parts of the system propagation of failure. Design flaws that require safeguards to insure operability (double valves, bypass redundance logic, manual overrides, etc.) can thus be uncovered. This method is used both in pre-design and post-design analyses to achieve design verification, set acceptance criteria, meet objectives in system operation, provide procedural modifications to ensure safe operation and emplace monitoring of safety critical items. A Haz-Op variant is LAD (Loss Analysis Diagram), used to compare design options and determine the risk acceptability levels or safety margins in design. Similarly, contingency analysis is used as a complementary risk analysis method to Haz-Op, in order to manage risks, when loss of control or a critical accident occurs.

In contrast to the above approaches, deductive risk analysis methods require reasoning from the general to the specific: A system failure is postulated and the subsystem failure modes leading to it are analyzed and broken down to the terminal or initiating failure event level ("top to bottom" or "top down" approach). Most accident investigations are of this type and are used to determine how a system failure can occur.[8] This includes:

- <u>The Fault Tree Analysis (FTA) Methodology for Hazard Assessment</u> - The FTA technique is a logical method for display and analysis of the hierarchical linkage and propagation of failure events leading to the adverse end result, placed at the top of the "tree." Branches in this logic tree represent alternative failure paths leading to the stipulated end event and display interdependencies of failures. A staged fault tree (Figure 8-7) allows the definition of intermediate levels of the events and conditions that are necessary or enable failures to propagate to the top of the tree. The intermediate failure events may, in turn, result from the aggregation of lower level failures from system-level down to subsystems and component failures. The bottom levels display the failure initiating or tree terminal events. Critical factors and interrupt modes for failure chains can be identified and quantitatively examined. The nodes of the fault tree represent logic AND or OR gates.



Legend: Faults
E_1 - Top event
$E_2 ... E_5$ intermediate fault event
R = primary failure
S, S_1 = primary failure
K_1, K_2 = primary failure
T = primary failure
Circles denote terminal events

Rectangles denote fault events requiring further branching development and analysis into sub events.

- OR gate with two independent input events, either of which can lead to failure, but which cannot occur simultaneously (plus denotes additive probabilities).

- AND gate specifies a causal failure where input faults jointly cause the output fault and the dot denotes a product of probabilities (both must occur for failure).

FIGURE 8-7. BASIC FAULT TREE SCHEMATIC (REF. 8)

The AND gate represents the simultaneous occurrence of conditions or events necessary to result in failure propagation up the tree. An OR gate indicates that each individual failure event entering is capable of leading to higher level failures. Careful consideration must be given to the independence or mutual interdependence of events entering a particular logic gate to insure the correct use of joint and conditional probability concepts.

In the case of ELV launch or orbital failures, a fault tree may be used to highlight single point (critical) failures and "common cause" (not independent) failures which must be "designed out" by redundancy or greater safety margins. Clever analysts use "exclusive OR gates," by defining mutually exclusive sets of failure events or aggregating lower level failure events into complementary groups to facilitate estimation of probability at each node of this event fault tree. FTA can be used both for qualitative, and for quantitative analysis of hazards. However, qualitative results must be combined with accurate failure rate data in order to achieve meaningful quantitative results.

Assuming independence of failures, there are five "minimal cut sets," i.e., intersection of events, whose probabilities are added at OR gates (provided that individual failure probabilities are very small so that probability products are negligible compared to their sum), and multiplied at the AND gate.

$$
\begin{aligned}
E_1 &= T + E_2 = \\
&= T + (K_2 + E_3) = \\
&= T + K_2 + (S \cdot E_4) = \\
&= T + K_2 + S \cdot (S_1 + E_S) = \\
&= T + K_2 + (S \cdot S_1) + S \cdot (K_1 + R) = \\
&= T + K_2 + (S \cdot S_1) + S \cdot (K_1 + S) \cdot R
\end{aligned}
$$

The minimal cut sets are T, K_2, $S \cdot S_1$, $S \cdot K_1$ and $S \cdot R$ (two singles and three doubles). The largest contribution to the probabilities will come from the single point failures T and K_2 (critical failures), since the small probabilities of occurrence for the individual failure events, S, S_1, K_1 and R, the product of their probabilities will make a very small, and possibly negligible, contribution to the final event probability. Probabilities of simultaneous failures at AND gates necessary for a higher level failure to occur, may be multiplied in some approximations only if conditional probabilities for interdependent failures are subtracted and the correct dimensionality is preserved. Usually, probabilities of independent events at OR gates are added, if P<1. Correct dimensionality must be observed for all types of logic gates.[8]

Each branch of a failure event tree must be quantified in a consistent manner using either frequency units (1/time dimensions, rate per year, per hour or per event) or normalized dimensionless probabilities. By using observed or projected/expected values for the frequency or probability of various failure modes and by analyzing how they occur, the likelihood of each hazardous event can be quantified. Risk is the product of this probability (or frequency) by the consequence magnitude of the undesirable event. The correct probabilistic dependencies (conditional, joint, mutually exclusive) for the occurrence of failure events of the lower branches permit their quantitative aggregation at gates and up the tree. References 1, 3, 7, 8 and 10 discuss and illustrate the application, use and practice of FTA and other Probabilistic Risk Analysis (PRA) methods, such as FMEA, in industry and Government.

The NRC and DOE have made extensive use of PRA in analyzing, licensing and regulating the operation of nuclear power plants; in prioritizing generic nuclear industry, transportation and waste disposal safety issues and in performing environmental impact analyses.[14-16] DOD has also used PRA to develop and test nuclear weapon systems. PRA is a comprehensive and integrated analysis of failures capable of revealing their interrelationship and their likelihood. Thus, in spite of its uncertainties, high cost, effort and limitations, PRA has proven useful to regulators of technological risk both to highlight gaps in knowledge and areas of research need and in directing the industry and regulatory efforts towards redress of high leverage safety problems. PRA's have aided in formulating safety goals, criteria and defining risk acceptability levels and numerical compliance targets for industry.

REFERENCES TO CHAPTER 8

1. "A Review of Risk Assessment Methodologies" - Report by the Congressional Research Service (CRS), Comm. on Sci. and Technology, Comm. Print 98-929 (1983)

2. "Risk Assessment in the Federal Government: Managing the Process," NAS (1983)

3. "Risk Assessment and Risk Management: Framework for Decision making," EPA Policy Paper, 1984; also "Science, Risk and Public Policy," W.D. Ruckelshaus, Science 221. 1026 (1983).

4. "The Perils of Prudence," A. L. Nichols and R. J. Zeckhauser, in "Regulation," Nov/Dec 1986, p. 13 et ag.

5. "The Dangers of Caution: Conservatism in Assessment and Management of Risk," A. L. Nichols & R. J. Zeckhauser, p. 5-582 in Advances in Appl. Micro- Economics, Vol. 4 on "Risk, Uncertainty and the Value of Benefits and Costs."

6. "Product Safety Management and Engineering," Willie Hammer, Prentice Hall Intl., 1980.

7. "System Safety Engineering and Management," H. E. Roland and B. Moriarty, J. Wiley & Sons, 1983.

8. "Fault Tree Handbook," NUREG-0492, Jan. 1981, Vesely, W., et. al.

9. "Social Benefits vs. Technological Risk," Chauncey Starr, Science 165, 1232 (Sept. 19, 1969).

10. "Hazard Identification and Quantification," H. Ozog and L. M. Bendixen, Chemical Engineering Progress, April 1987, p. 55-64.

11. "Inferences from Alarming Events," J. W. Pratt and R. J. Zeckhauser, J. Policy Analysis and Mgt., 1, 321 (1982).

12. "Computing Risk Profiles for Composite Low Probabilty High Consequence Events," D. J. Heimann and T. S. Glickman, Annals of Operations Res. (1987), 9, 545-560 (1987) in "Statistical and Computational Issues in Probability Modeling II, (eds. S. L. Albin and C. M. Harris).

13. "Review of RTG Utilization in Space Missions," Hearing, House Comm. on Sci. & Tech., March 4, 1986 (Rept. # 97), see Testimony and Appendices (esp. pp. 252, 280, et seq.).

14. "Risk Management Guide", G.J. Briscoe, EG&G, Idaho, for DOE, DOE/SSDC-76- 45/11- Rev.1, Sept. 1982.

15. "Probabilistic Risk Assessment (PRA) Reference Document," NRC, NUREG- 1050-F, Sept. 1984.

16. "PRA Procedures Guide- A guide for the Performance of Probabilistic risk assessments for Nuclear power plants," NRC, NUREG-CR-2300, 1981.

17. "An Anatomy of Risk," W.D. Rowe,J.Wiley and Sons, New York, 1977; Second Ed., 1986.

18. "Methodologies for Hazard Analysis and Risk Assessment in the Petroleum Refining and Storage Industry," Concawe, Report 10-82, 1982.

19. "Regulatory Program of the US Government, April 1, 1986 - March 31, 1987," Exec. Off. of the President, OMB, (p. xx, T.2).